PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-067399
(43)Date of publication of application : 16.03.2001

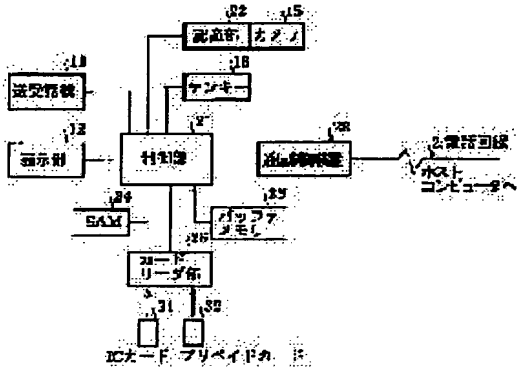
(51)Int.Cl. G06F 17/60
G06F 19/00
G06T 7/00
G07D 9/00
H04M 3/42
H04M 11/00
H04M 15/00

(21)Application number : 11-237667
(22)Date of filing : 25.08.1999

(71)Applicant : OKI ELECTRIC IND CO LTD
(72)Inventor : TAKIZAWA TOSHIO

(54) ELECTRONIC MONEY TRANSACTION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To load the electronic money by means of a general telephone circuit.
SOLUTION: In this electronic money transaction system, the irises of an operator of a public telephone set are photographed by a camera 15 and recognized at a recognition part 22. Meanwhile, the personal information stored in an IC card 31 is read at a card reader part 26. The card 31 stores the registered two iris data and a control part 21 compares these iris data with each other to authenticate the identity of the operator. When this identity is authenticated, the loaded amount of electronic money is inputted to generate the communication data including the loaded amount. The communication data are enciphered and then transmitted to a host computer via a telephone circuit 2.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (JP)　　(12) 公開特許公報（A）　　(11) 特許出願公開番号

特開２００１－６７３９９
（Ｐ２００１－６７３９９Ａ）
(43) 公開日　平成13年3月16日 (2001. 3. 16)

(51) Int. Cl.⁷		識別記号	FI			テーマコード (参考)
Ｇ０６Ｆ	17/60		Ｇ０６Ｆ	15/21	３４０　Ｚ	3E040
	19/00		Ｇ０７Ｄ	9/00	４６１　Ａ	5B043
Ｇ０６Ｔ	7/00		Ｈ０４Ｍ	3/42	Ｚ	5B049
Ｇ０７Ｄ	9/00	４６１		11/00	３０２	5B055
Ｈ０４Ｍ	3/42			15/00	Ｚ	5K024

審査請求　未請求　請求項の数９　ＯＬ　（全１２頁）　最終頁に続く

(21) 出願番号　特願平11-237667

(22) 出願日　平成11年8月25日 (1999. 8. 25)

(71) 出願人　000000295
沖電気工業株式会社
東京都港区虎ノ門1丁目7番12号

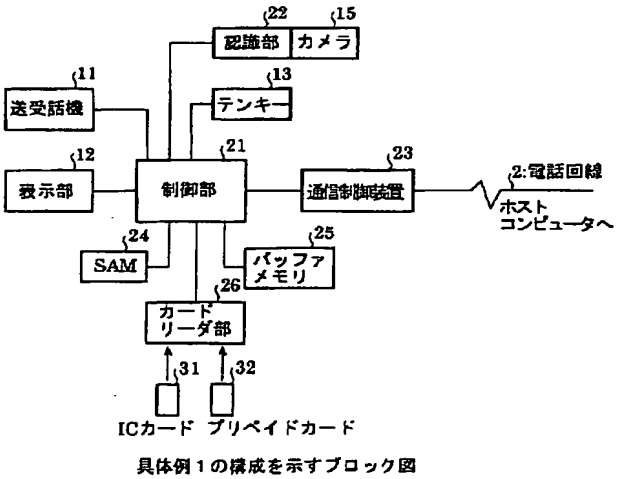
(72) 発明者　滝沢　俊男
東京都港区虎ノ門1丁目7番12号　沖電気工業株式会社内

(74) 代理人　100082050
弁理士　佐藤　幸男

最終頁に続く

(54) 【発明の名称】電子マネー取引システム

(57) 【要約】
【課題】　一般の電話回線２を用いて電子マネーのローディングを行う。
【解決手段】　公衆電話機の操作者の目のアイリス（虹彩）をカメラ１５により撮影し、認識部２２で認識する。また、ＩＣカード３１に格納されている個人情報をカードリーダ部２６を用いて読み取る。このＩＣカード３１には、登録されたアイリスデータが格納されており、制御部２１では、この２つのアイリスデータを比較して本人認証を行う。本人を認証できたときは、電子マネーのロード金額を入力し、このロード金額を含めて通信データを生成し、暗号化した後、電話回線２を介してホストコンピュータへ送信する。



具体例１の構成を示すブロック図

1

【特許請求の範囲】

【請求項１】　金融機関の取引対象者が操作する端末と金融機関のホストコンピュータとの間で、通信回線を介して電子マネーによる取引を行う電子マネー取引システムにおいて、

前記通信回線に電話回線を用いるとともに、情報の読み書きが可能なものであって中央演算装置及び記憶手段を内蔵したＩＣカードに、取引対象者のバイオメトリクス情報を登録する一方、

前記端末は、ＩＣカードの真偽を判定するＩＣカード認証手段と、

該ＩＣカード認証手段によりＩＣカードが真と判定されたとき、ＩＣカードに格納されている情報を読み取る情報読み取り手段と、

端末を操作して取引要求を行った操作者から、当該操作者のバイオメトリクス情報を取得するバイオメトリクス情報取得手段と、

前記バイオメトリクス情報取得手段によって取得されたバイオメトリクス情報と情報読み取り手段によって読み出された情報のうちのバイオメトリクス情報とを比較して、端末の操作者がＩＣカードに登録された取引対象者本人であるか否かを認証する本人認証手段と、

該本人認証手段により、取引対象者本人であることが認証されたとき、電子マネーによる取引を受け付けて取引要求情報を入力する取引要求情報入力手段と、

該取引要求情報入力手段によって入力された取引要求情報を含む情報に対し、セキュリティ処理を行って通信データを生成し、電話回線を介して該通信データをホストコンピュータに送信する端末側送信手段と、

送信した通信データに対応してホストコンピュータから返信データが返信されたとき、該返信データから取引の処理結果を示す取引処理情報を取り出す端末側受信手段と、を備え、

前記ホストコンピュータは、端末からの通信データを受信して該通信データから取引要求情報を取り出すホスト側受信手段と、

該ホスト側受信手段により取り出された取引要求情報に基づいて取引に関する処理を行う取引処理手段と、

該取引処理手段によって処理されて出力された取引処理結果を含む情報に対し、セキュリティ処理を行って返信データを生成し、通信データの送信元端末に、電話回線を介して該返信データを送信するホスト側送信手段と、を備えたことを特徴とする電子マネー取引システム。

【請求項２】　前記バイオメトリクス情報は、取引対象者及び操作者の目の虹彩画像の情報であることを特徴とする請求項１に記載の電子マネー取引システム。

【請求項３】　前記ＩＣカードに接続先ホストコンピュータの電話番号を記録し、前記端末の情報読み取り手段は、ＩＣカードから当該電話番号を読み取り、端末側送信手段は、読み取られた電話番号に基づいて接続先ホストコンピュータに接続し、通信データを送信するように構成されたことを特徴とする請求項１又は請求項２に記載の電子マネー取引システム。

2

【請求項４】　前記ＩＣカード及びホストコンピュータに、それぞれ対応する通信用暗号鍵及び通信用復号鍵を格納する一方、

前記端末の情報読み取り手段は、ＩＣカードから通信用暗号鍵を読み取り、端末側送信手段は、セキュリティ処理として、ＩＣカードから読み取った通信用暗号鍵を用いて情報の暗号化を行い、前記端末側受信手段は、ＩＣカードから読み取った復号鍵を用いてホストコンピュータから送信された返信データの復号化を行うように構成され、

前記ホストコンピュータのホスト側受信手段は、セキュリティ処理として、格納された通信用復号鍵を用いて端末から送信された通信データの復号化を行い、前記ホスト側送信手段は、格納された通信用暗号鍵を用いて情報の暗号化を行うように構成されたことを特徴とする請求項１～請求項３のいずれか１つに記載の電子マネー取引システム。

【請求項５】　前記ＩＣカードに、ＩＣカード固有のカードＩＤを格納し、前記端末の情報読み取り手段は、当該カードＩＤを読み取り、読み取ったカードＩＤを用いてＩＣカードに格納された通信用暗号鍵及び通信用復号鍵を読み取るように構成されたことを特徴とする請求項４に記載の電子マネー取引システム。

【請求項６】　前記カードＩＤは暗号化されたものであることを特徴とする請求項５に記載の電子マネー取引システム。

【請求項７】　前記ホストコンピュータは、暗号化されたカードＩＤを復号化するカードＩＤ復号鍵を格納する一方、

前記端末の端末側送信手段は、暗号化されたカードＩＤを通信データに含めてホストコンピュータに送信するように構成され、

前記ホスト側受信手段は、通信データから暗号化されたカードＩＤを取り出し、ホストコンピュータに格納されたカードＩＤ復号鍵を用いてカードＩＤの復号化を行い、該復号化されたカードＩＤを用いてホストコンピュータに格納された通信用復号鍵を取り出すように構成され、

前記ホスト側送信手段は、ホスト側受信手段によって復号化されたカードＩＤを用いてホストコンピュータに格納された通信用暗号鍵を取り出すように構成されたことを特徴とする請求項６に記載の電子マネー取引システム。

【請求項８】　前記端末は、公衆電話機であることを特徴とする請求項１～請求項７のいずれか１つに記載の電子マネー取引システム。

【請求項９】　前記端末は、パーソナルコンピュータで

あることを特徴とする請求項１～請求項７のいずれか１つに記載の電子マネー取引システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ＩＣカード、バイオメトリクス情報を利用してオフラインで認証を行い、電話回線を介して電子マネーの取引を行う電子マネー取引システムに関する。

【０００２】

【従来の技術】従来の電子マネー取引システムでは、不正を防止するため、暗証番号を用いて取引対象者の本人認証を行うようにしている。

【０００３】しかし、この暗証番号を用いたシステムにおいて、セキュリティ性を向上させるためには、ハードウェア、ソフトウェアを含めてシステム上、高価なものになってしまう。そこで、近年、本人特有のバイオメトリクス情報を用いて本人認証を行うシステムが開発されている。

【０００４】

【発明が解決しようとする課題】しかしながら、このようなバイオメトリクス情報を用いて本人認証を行う従来の電子マネー取引システムにおいても、セキュリティ性を高めるためには、専用の回線を用いて電子マネーのローディングを行う必要があり、いつでもどこでもかかるローディングを手軽に行うというわけにはいかず、通信コストも低減させることは困難であった。従って、一般の電話回線を用いて電子マネーのローディングを行えるようになれば、容易に電子マネーによる取引を行えるようになる。

【０００５】

【課題を解決するための手段】本発明は以上の点を解決するため次の構成を採用する。

〈構成１〉請求項１の発明に係る電子マネー取引システムは、金融機関の取引対象者が操作する端末と金融機関のホストコンピュータとの間で、通信回線を介して電子マネーによる取引を行う電子マネー取引システムにおいて、前記通信回線に電話回線を用いるとともに、情報の読み書きが可能なものであって中央演算装置及び記憶手段を内蔵したＩＣカードに、取引対象者のバイオメトリクス情報を登録する一方、前記端末が、ＩＣカードの真偽を判定するＩＣカード認証手段と、該ＩＣカード認証手段によりＩＣカードが真と判定されたとき、ＩＣカードに格納されている情報を読み取る情報読み取り手段と、端末を操作して取引要求を行った操作者から、当該操作者のバイオメトリクス情報を取得するバイオメトリクス情報取得手段と、前記バイオメトリクス情報取得手段によって取得されたバイオメトリクス情報と情報読み取り手段によって読み出された情報のうちのバイオメトリクス情報とを比較して、端末の操作者がＩＣカードに登録された取引対象者本人であるか否かを認証する本人認証手段と、該本人認証手段により、取引対象者本人であることが認証されたとき、電子マネーによる取引を受け付けて取引要求情報を入力する取引要求情報入力手段と、該取引要求情報入力手段によって入力された取引要求情報を含む情報に対し、セキュリティ処理を行って通信データを生成し、電話回線を介して該通信データをホストコンピュータに送信する端末側送信手段と、送信した通信データに対応してホストコンピュータから返信データが返信されたとき、該返信データから取引の処理結果を示す取引処理情報を取り出す端末側受信手段と、を備え、前記ホストコンピュータが、端末からの通信データを受信して該通信データから取引要求情報を取り出すホスト側受信手段と、該ホスト側受信手段により取り出された取引要求情報に基づいて取引に関する処理を行う取引処理手段と、該取引処理手段によって処理されて出力された取引処理結果を含む情報に対し、セキュリティ処理を行って返信データを生成し、通信データの送信元端末に、電話回線を介して該返信データを送信するホスト側送信手段と、を備えたものである。

【０００６】〈構成２〉請求項２の発明に係る電子マネー取引システムでは、前記バイオメトリクス情報が取引対象者及び操作者の目の虹彩画像の情報である。

【０００７】〈構成３〉請求項３の発明に係る電子マネー取引システムでは、前記ＩＣカードに接続先ホストコンピュータの電話番号を記録し、前記端末の情報読み取り手段が、ＩＣカードから当該電話番号を読み取り、端末側送信手段が、読み取られた電話番号に基づいて接続先ホストコンピュータに接続し、通信データを送信するように構成されている。

【０００８】〈構成４〉請求項４の発明に係る電子マネー取引システムでは、前記ＩＣカード及びホストコンピュータに、それぞれ対応する通信用暗号鍵及び通信用復号鍵を格納する一方、前記端末の情報読み取り手段が、ＩＣカードから通信用暗号鍵を読み取り、端末側送信手段が、セキュリティ処理として、ＩＣカードから読み取った通信用暗号鍵を用いて情報の暗号化を行い、前記端末側受信手段が、ＩＣカードから読み取った復号鍵を用いてホストコンピュータから送信された返信データの復号化を行うように構成され、前記ホストコンピュータのホスト側受信手段が、セキュリティ処理として、格納された通信用復号鍵を用いて端末から送信された通信データの復号化を行い、前記ホスト側送信手段が、格納された通信用暗号鍵を用いて情報の暗号化を行うように構成されている。

【０００９】〈構成５〉請求項５の発明に係る電子マネー取引システムでは、前記ＩＣカードに、ＩＣカード固有のカードＩＤを格納し、前記端末の情報読み取り手段が、当該カードＩＤを読み取り、読み取ったカードＩＤを用いてＩＣカードに格納された通信用暗号鍵及び通信用復号鍵を読み取るように構成されている。

【００１０】〈構成６〉請求項６の発明に係る電子マネー取引システムでは、前記カードＩＤが暗号化されたものである。

【００１１】〈構成７〉請求項７の発明に係る電子マネー取引システムでは、前記ホストコンピュータが、暗号化されたカードＩＤを復号化するカードＩＤ復号鍵を格納する一方、前記端末の端末側送信手段が、暗号化されたカードＩＤを通信データに含めてホストコンピュータに送信するように構成され、前記ホスト側受信手段が、通信データから暗号化されたカードＩＤを取り出し、ホストコンピュータに格納されたカードＩＤ復号鍵を用いてカードＩＤの復号化を行い、該復号化されたカードＩＤを用いてホストコンピュータに格納された通信用復号鍵を取り出すように構成され、前記ホスト側送信手段が、ホスト側受信手段によって復号化されたカードＩＤを用いてホストコンピュータに格納された通信用暗号鍵を取り出すように構成されている。

【００１２】〈構成８〉請求項８の発明に係る電子マネー取引システムでは、前記端末が公衆電話機である。

【００１３】〈構成９〉請求項９の発明に係る電子マネー取引システムでは、前記端末がパーソナルコンピュータである。

【００１４】

【発明の実施の形態】以下、本発明の実施の形態を具体例を用いて説明する。

〈具体例１〉具体例１は、ＩＣカードを用い、通信回線として電話回線を用いて端末としての公衆電話機から電子マネーのローディングを行うようにしたものである。

【００１５】図１は、具体例１の構成を示すブロック図であり、図２は、図１の構成を内蔵した公衆電話機１の外観を示す斜視図である。図２に示すように、公衆電話機１の側面には送受話器１１が備えられ、前面パネルには、表示部１２、テンキー１３、ＩＣカード挿入口１４及びレシート排出口１６が配置されている。

【００１６】テンキー１３は、例えば１２個のキーを備え、相手の電話番号及び電子マネーのロード金額を入力するのに使用する取引要求情報入力手段である。表示部１２は、例えば液晶を用いた表示部であり、文字のほか、イメージも表示できるものである。

【００１７】この表示部１２の上部には、バイオメトリクス情報取得手段としてのカメラ１５が配置されている。このカメラ１５は、ＣＣＤ（charge coupled device：電荷結合素子）を備え、操作者の目を撮影してバイオメトリクス情報としての虹彩（アイリス）の画像を得るためのものである。

【００１８】虹彩は眼球の角膜と水晶体との間にあり、中央に瞳孔を有する薄膜である。この虹彩は、瞳孔の開閉をコントロールして眼球内に入る光の量を調節するものであり、幼年期に完成され、各人毎によって異なるパターンを有している。このパターンは右目と左目とでも相違するが、一生を通じてほとんど変化することはない。従って、虹彩の情報は、まさに本人しか保有できない有力なバイオメトリクス情報となる。

【００１９】尚、バイオメトリクス情報としては、虹彩に限られるものではなく、サイン、網膜、声紋、顔貌、指紋、手形の情報を用いることもできる。サイン、声紋、顔貌、指紋、手形の情報を用いるときは、カメラ１５の代わりに、これらの情報を得ることのできるバイオメトリクス情報取得手段を用いる。但し、この虹彩パターンを用いれば、サインや指紋、声紋等と比較して少ないデータ量で本人認証を行うことができるので、有利である。レシート排出口１６はレシートを排出する出口であるが、これはオプションである。

【００２０】図３は　具体例１のシステム構成図である。ネットワーク３は、銀行５のホストコンピュータが接続されたネットワークであり、ネットワーク４は、カード会社６のコンピュータが接続されたネットワークである。公衆電話機１は電話回線２、ネットワーク３を介して銀行５のホストコンピュータに、さらにネットワーク４を介してカード会社６のホストコンピュータに接続されている。そして、銀行カード決済のときは、公衆電話機１と銀行５のホストコンピュータとの間で電子マネーのローディングが行われ、クレジットカード決済のときは、公衆電話機１とカード会社６のホストコンピュータとの間で電子マネーのローディングが行われる。

【００２１】この公衆電話機１は、図１に示すように、制御部２１と、通信制御装置２３と、認識部２２と、ＳＡＭ（Security Application Module）２４と、バッファメモリ２５と、カードリーダ部２６とを内蔵している。

【００２２】制御部２１は、マイクロコンピュータ、周辺ＲＯＭ、ＲＡＭ、Ｉ／Ｏとのインタフェース等を備えて構成され、送受話器１１、表示部１２、テンキー１３等もこの制御部２１に接続されている。そして、制御部２１は、公衆電話機１を制御し、後述するフローチャートに従って電子マネーのロードを実行する。

【００２３】認識部２２は、カメラ１５と接続され、カメラ１５によって捕らえられた操作者の目の画像に基づいて、目の虹彩（アイリス）の画像のデジタルデータを作成し、このデジタルデータを一旦蓄積し、このデータと別のデータとで本人であるかどうかの認証処理を行うためのものである。

【００２４】ＳＡＭ２４は、ＩＣカード３１の真偽を認証するために使用するＩＣカード認証手段であり、ＩＣカード３１とほぼ同一の構成を有している。通信用のバッファメモリ２５は、送受信する情報を一旦ストアしておくためのものである。

【００２５】通信制御装置２３は、モデム／ＮＣＵ等を備え、通信制御を行う装置であり、電話回線２、ＩＳＤＮ回線を経由して銀行５又はカード会社６のホストコン

ピュータに接続される。

【００２６】カードリーダ部２６は、ＩＣカード３１、例えばテレホンカードのようなプリペイドカードを受け付けて、データをリードライトする情報読み取り手段である。尚、プリペイドカードはオプションである。

【００２７】ＩＣカード３１は、そのカード基材にＩＣ（集積回路）チップを埋め込んで構成されたカードであり、このＩＣカード３１に取引対象者本人の個人情報が記録される。このＩＣカード３１のＩＣチップには、ＣＰＵ（中央演算装置）、各種処理プログラムが書き込まれたＲＯＭ（Read Only Memory）、取引内容等を一時的に記憶するためのＲＡＭ（Random Access Memory）、電気的に記憶情報の消去、書き込みが可能な不揮発性メモリであるＥＥＰＲＯＭ（Electrically Erasable andProgrammable ROM）が設けられている。さらにこのＩＣチップには、データを記憶させるための記憶回路、そして、これらの各メモリの情報の読み取り、書き込みを制御する制御回路も一体に形成されている。このＩＣカード３１の表面には、ＩＣチップに接続された端子部が露出し、この端子部を介して情報の読み書きが行われる。尚、近年、ＩＳＯ１０５３６やＩＳＯ１４４４３に公開されているように、接触部のないＩＣカードも開発されており、このような非接触型ＩＣカードでも同様に用いることができる。

【００２８】図４は具体例１のＩＣカード３１のファイル構成を示す説明図である。ＩＣカード３１に格納されたファイルは階層化され、マスタファイルの下に複数の専用ファイルがあり、さらにその下にエレメンタリファイルがある。このエレメンタリファイル１には、カードＩＤ、個人名、アイリスデータ、暗証番号用暗号鍵、ロード金額、接続電話番号、口座番号、ロード金額復号鍵、カードＩＤ復号鍵等の個人情報が記録され、エレメンタリファイル２には、通信用暗号鍵、通信用復号鍵が記録されている。

【００２９】尚、カードＩＤは、通信用暗号鍵、通信用復号鍵の情報を読み取るときに用いる情報であり、セキュリティ性を高めるため、暗号化されている。また、アイリスデータは前述の虹彩パターンに関するデータであり、そのデータサイズは、例えば２５６バイトである。

【００３０】このＩＣカード３１は、ＩＣカード３１の破損を避けるため、接続端子がＩＣカード挿入口１４の端子（図示せず）に接続されるまで、非活性化され、データの読み書きができないようになっている。このＩＣカード３１にデータの読み書きを行うためには、ＪＩＳ規格ＪＩＳＸ６３０６に規定されている手順に従ってＩＣカード３１を活性化させる必要がある。

【００３１】図５は、銀行５又はカード会社６のホストコンピュータの構成を示すブロック図である。ホストコンピュータ４１は、ファイル４２～４４を備えている。ファイル４２は、ログ用ファイルであり、ファイル４３は、カードＩＤの復号鍵を格納したファイルであり、ファイル４４は、通信用暗号鍵、通信用復号鍵、暗証番号用復号鍵を格納したファイルである。

【００３２】〈具体例１の動作〉図６及び図７は具体例１の動作を示すフローチャートである。ステップ（図中、「Ｓ」と記す。）１では、操作者が、自分のＩＣカード３１へ電子マネーを充填するためにＩＣカード３１をＩＣカード挿入口１４に挿入し、このＩＣカード３１を吸い込む。

【００３３】ステップ２では、ＳＡＭ２４を用いて相互認証を行い、ＩＣカード３１の真偽を判定する。相互認証は、ＩＣカードのＪＩＳ規格ＪＩＳＸ６３０６に規定されているＥＸＴＥＲＮＡＬ　ＡＵＴＨＥＮＴＩＣＡＴＥコマンド、あるいはＩＮＴＥＲＮＡＬＡＵＴＨＥＮＴＩＣＡＴＥコマンドを使い、暗号技術を用いて行われる。ＥＸＴＥＲＮＡＬ　ＡＵＴＨＥＮＴＩＣＡＴＥコマンドは、ＩＣカード３１外部で暗号化し、ＩＣカード３１内で認証結果を計算させるときに用いられるコマンドであり、ＩＮＴＥＲＮＡＬ　ＡＵＴＨＥＮＴＩＣＡＴＥコマンドは、外部から種となる情報、例えば乱数を与えて暗号化し、その認証結果を外部で判断するときに用いられるコマンドである。相互認証中、公衆電話機１の表示部１２にメッセージが表示される。

【００３４】図８は、表示部１２に表示するメッセージの表示例を示す説明図である。この図８（Ａ）に示すように、相互認証中、表示部１２には「カード認証中」「しばらくお待ち下さい」とのメッセージが表示される。そして、カードが真と認証されたときは、ステップ３に進む。ステップ３では、カメラ１５を用いて操作者の目を撮影し、操作者のアイリス画像を取り込む。

【００３５】このとき、図８（Ｂ）に示すように、「あなたの確認を致します。」「矢印の先のレンズをご覧下さい」とのメッセージを表示させ、操作者の注意を引くようにする。そして、できるだけ目線を表示部１２に集中させるため、矢印を点滅等させる。認識部２２は、取り込んだアイリス画像をデジタルデータに変換し、２５６バイトのアイリスデータを得る。

【００３６】ステップ４では、ＩＣカード３１から、登録されているアイリスデータを読み取る。読み取りは、カードリーダ部２６によって行われる。このアイリスデータは、図４に示すようにエレメンタリファイルに格納されている。

【００３７】ステップ５では、カメラ１５から取り込んだアイリスデータとＩＣカード３１から読み取ったアイリスデータとを比較して本人の認識を行う。このアイリス認証には、例えば米国特許第５，２９１，５６０号公報に開示された技術を用いる。本人を認証できたときは、ステップ８に進む。

【００３８】また、本人を認証できなかったときはステップ６に進み、所定のリトライ回数、例えば３回以下で

あるか否かを判定する。リトライ回数が３回以下のときは、ステップ３に戻り、再び本人の認証を行う。このとき、表示部１２に、もう一度操作者に本人の認証を行う旨のメッセージを表示させる。

【００３９】リトライ回数が３回以下で本人を認証できたときは、ステップ８に進む。また、リトライ回数が３回を超えたときは、操作者は、取引対象者本人ではないと判定してステップ７に進み、取引の停止処理を行う。このとき、操作者に暗証番号を入力させ、確認するようにしてもよい。暗証番号が入力されたときは、ＩＣカード３１に格納されている暗証番号用暗号鍵を用いて暗号化される。

【００４０】ステップ８では、ＩＣカード３１に対し、ＲＥＡＤコマンドを発行し、ＩＣカード３１のエレメンタリファイル１に格納されている個人情報等及びエレメンタリファイル２に格納されている通信用暗号鍵、通信用復号鍵を直接読み取る。尚、通信用暗号鍵、通信用復号鍵を直接読み取ることはできず、カードＩＤが必要である。また、このカードＩＤは暗号化されているため、これらの鍵情報を読み取るには、まず、エレメンタリファイル１からカードＩＤ復号鍵を取り出して、このカードＩＤを復号化する。そして、この復号化されたカードＩＤを用いてエレメンタリファイル２に格納されている通信用暗号鍵、通信用復号鍵を読み取る。このようにしてセキュリティ性を高めている。

【００４１】ステップ９では、読み取った個人情報をバッファメモリ２５に格納する。ステップ１０では、図８（Ｃ）に示すように、「ロード金額を入力して下さい」とのメッセージを表示部１２に表示させ、操作者に取引要求情報としてロード金額の入力を促す。操作者は、このメッセージに従ってテンキー１３を用い、所定のロード金額を入力する。ステップ１１では、入力されたロード金額をバッファメモリ２５に格納し、通信データを生成する。

【００４２】図９は、具体例１の前半の動作を示す動作説明図である。この図９（Ａ）に示すように、この通信データには、カードＩＤ、口座番号、ロード要求金額、暗証番号、アイリスデータ等が含まれ、この先頭部にヘッダ、後端にはエンドデータが付加される。

【００４３】ステップ１２では、図９（Ｂ）に示すように、バッファメモリ２５に格納された通信データのうち、口座番号、ロード要求金額、暗証番号、アイリスデータ等のデータを暗号化する。尚、暗証番号は、ステップ７において入力されるオプションデータであり、暗証番号があるときは、二重に暗号化されることになる。これによってセキュリティ性が高められる。

【００４４】この暗号化は、ＩＣカード３１から読み取られた通信用暗号鍵を用いて行われる。暗号方式としては共通鍵方式のＤＥＳ（Data Encryption Standard）、公開鍵方式のＲＳＡ等を用いるのが一般的であるが、この方式に限られるものではない。

【００４５】ステップ１３では、ＩＣカード３１から読み取った接続電話番号を用いてホストコンピュータ４１に接続し、この通信データを送信する。但し、テンキー１３を用いて接続先ホストコンピュータの電話番号を入力することもできる。

【００４６】ステップ１４～１６は、ホストコンピュータ４１によって実行される。ステップ１４では、図９（Ｃ）に示すように、受信した通信データを復号化する。

【００４７】通信データを復号化するには、まず、暗号化されたカードＩＤを通信データから取り出し、このカードＩＤを、ファイル４３に格納されているカードＩＤの復号鍵を用いて復号化する。そして、復号化されたカードＩＤの番号をキーとしてファイル４４を検索し、ファイル４４から通信用復号鍵と暗証番号用復号鍵を取り出す。さらに、この通信用復号鍵を用いて通信データを復号化する。尚、暗号化された暗証番号が含まれているときは、暗証番号用復号鍵を用いてこの暗証番号を復号化する。

【００４８】このように公衆電話機１から送信されたカードＩＤを用いてファイル４４から通信用復号鍵と暗証番号用復号鍵を取り出すようにしたので、このカードＩＤを分からなければこれらの復号鍵を取り出すことができず、セキュリティ性が保証される。

【００４９】ステップ１５では、ホストコンピュータ４１が所定の処理を行う。図１０は、具体例１の後半の動作を示す動作説明図である。このホストコンピュータ４１の処理により、図１０（Ａ）に示すように、復号化された通信データから口座番号とロード要求金額が取り出され、口座番号に基づいて電子マネーが引き出される。処理終了後、口座番号、ロード金額及びアイリスデータはログ用のファイル４２へ記録され、トランザクションが残る。トランザクションを残すことにより、確実に口座を有する取引対象者本人に対して金額をロードしたという証拠が残る。

【００５０】ステップ１６では、図１０（Ｂ）に示すように、カードＩＤ、口座番号及びロード金額が格納された通信データを形成し、ファイル４４から取り出された通信用暗号鍵を用いてこの口座番号とロード金額を暗号化し、図１０（Ｃ）に示すような通信データを生成する。尚、この通信用暗号鍵は、前述の復号化したカードＩＤの番号をキーとして取り出される。生成された通信データは、送信元の公衆電話機１に送信され、公衆電話機１は、ステップ１７～１９を実行する。

【００５１】ステップ１７では、図１０（Ｄ）に示すように、通信データを受信し、ＩＣカード３１から読み取った通信用復号鍵を用いて復号化する。その結果、図１０（Ｅ）に示すような通信データが得られる。そして、ＷＲＩＴＥコマンドを発行し、この通信データに格納さ

れているロード金額情報を、ＩＣカード３１のエレメンタリファイルのロード金額エリアに格納する。

【００５２】ステップ１８では、図８（Ｄ）に示すように、「ありがとうございました」とのメッセージを表示させるとともに、取引日付、口座番号、ロード金額、取引通番を表示部１２の画面に表示させる。表示後、ＩＣカード３１を非活性化させるとともに、ＩＣカード３１をＩＣカード挿入口１４からリリースする。

【００５３】ステップ１９では、結果をレシートに印刷し、このレシートをレシート排出口１６から排出する。尚、ステップ５が本人認証手段に、ステップ１２及び１３が端末側送信手段に、ステップ１４がホスト側受信手段に、ステップ１５が取引処理手段に、ステップ１６がホスト側送信手段に、ステップ１７が端末側受信手段に相当する。

【００５４】〈具体例１の効果〉以上、説明したように具体例１によれば、端末として公衆電話機１を利用し、電話回線２を用いて電子マネーのローディングを行うようにしたので、一般の電話回線２が接続された公衆電話機１があれば、専用の回線を用いることなくいつでもどこでも通信できる。このため、通信コストを低減することができる。

【００５５】また、ＩＣカード３１を用いてオフラインで本人認証を行い、電子マネーをロードするようにしたので、ホスト側に負荷をかけずに本人認証を行うことができ、しかも安全に電子マネーをロードすることができる。また、本人特有のアイリスデータを用いて電子マネーをロードするようにしたので、本人以外の他人によって電子マネーを引き出すという不正行為を防止することができ、セキュリティ上、万全なシステムを構築することができる。

【００５６】また、ＩＣカード３１から通信用暗号鍵、復号鍵を読み取り、この２つの鍵を用いて通信データの暗号化、ホストコンピュータ４１からの返信データの復号化を行い、さらに、このカードＩＤを用いて２つの鍵を読み取るとともに、このカードＩＤも暗号化するようにしたので、一般の電話回線２を用いた場合でも安全に通信を行うことができる。

【００５７】また、この暗号化されたカードＩＤをホストコンピュータ４１に送信し、このカードＩＤを復号化し、このカードＩＤを用いてファイル４４から通信用暗号鍵等を取り出すようにして、このカードＩＤを知らない第三者によって簡単に通信用暗号鍵等を取り出せないようにしたので、セキュリティ性が向上する。

【００５８】また、公衆電話機１からホストコンピュータ４１に通信データを送信するとき、ＩＣカード３１から読み取った接続電話番号を用いて自動的にホストコンピュータ４１に接続するようにしたので、操作者の負担を低減することができる。

【００５９】さらに、ホストコンピュータ４１側では、口座から引き落とす処理を行う場合に、操作者のアイリスデータを登録してトランザクションを残すようにしたので、本人が電子マネーのロードを行ったという証拠を残すことができ、万が一、犯罪等が発生したときに、その解決に役立てることができる。

【００６０】尚、本具体例１では、ステップ７において、暗証番号をオプションとして入力するようにしたが、暗証番号を入力させ、アイリスデータと暗証番号とを併用して本人認証を行うようにしてもよい。また、この暗証番号については、二重に暗号化するようにしたが、セキュリティ性が保証されれば、暗証番号用暗号鍵による暗号化を省略することもできる。

【００６１】〈具体例２〉具体例２は、端末としてパーソナルコンピュータを用い、このパーソナルコンピュータに電話回線を接続し、パーソナルコンピュータから電子マネーのローディングを行うようにしたものである。

【００６２】図１１は、具体例２の構成を示すブロック図であり、図１２は、図１１の構成を備えたシステムの外観を示す説明図である。図１２に示すように、パーソナルコンピュータ５１は、例えば液晶表示のディスプレイ５２と、キーボード５３とを備え、さらにディスプレイ５２の上部にカメラ５４を備えたノート型のパーソナルコンピュータである。

【００６３】このパーソナルコンピュータ５１には、所定のデータを入力するためのマウス５５と、ＩＣカード３１へのデータの読み書きを行うためのＩＣカードリーダライタ５６と、電話回線２とが接続されている。

【００６４】図１１に示すように、ディスプレイ５２、マウス５５、キーボード５３は、制御部２１に接続されている。具体例２では、ＳＡＭ２４がＩＣカードリーダライタ５６に内蔵されている。尚、具体例１と同一要素については同一符号を付して説明を省略する。

【００６５】〈動作〉パーソナルコンピュータ５１を用いて電子マネーのローディングを行うときは、ＩＣカード３１をＩＣカードリーダライタ５６に挿入する。挿入後、ＩＣカード３１とＩＣカードリーダライタ５６に内蔵されたＳＡＭ２４との間で相互認証が行われる。そして、具体例１と同じように電子マネーのローディングが行われる。

【００６６】〈具体例２の効果〉以上、説明したように具体例２によれば、汎用性のあるパーソナルコンピュータ５１を利用して電子マネーのローディングを行うようにしたので、電話回線２があれば、家庭でもオフィスでもいつでもどこでも手軽に、電子マネーのロードを行うことができる。

【００６７】尚、本具体例２では、ノート型のパーソナルコンピュータを利用した場合について説明したが、これに限られるものではなく、スタンドアローン型のパーソナルコンピュータを利用することもできる。

【図面の簡単な説明】

13

【図１】本発明の具体例１の構成を示すブロック図である。

【図２】具体例１の公衆電話機の外観を示す斜視図である。

【図３】具体例１のシステム構成図である。

【図４】具体例１のＩＣカード３１のファイル構成を示す説明図である。

【図５】ホストコンピュータの構成を示すブロック図である。

【図６】具体例１の動作を示すフローチャート（その１）である。

【図７】具体例１の動作を示すフローチャート（その２）である。

【図８】表示部に表示するメッセージの表示例を示す説明図である。

14

【図９】具体例１の動作説明図（その１）である。

【図１０】具体例１の動作説明図（その２）である。

【図１１】具体例２の構成を示すブロック図である。

【図１２】具体例２のシステムの外観を示す説明図である。

【符号の説明】

１　公衆電話機

２　電話回線

１５、５４　カメラ

２１　制御部

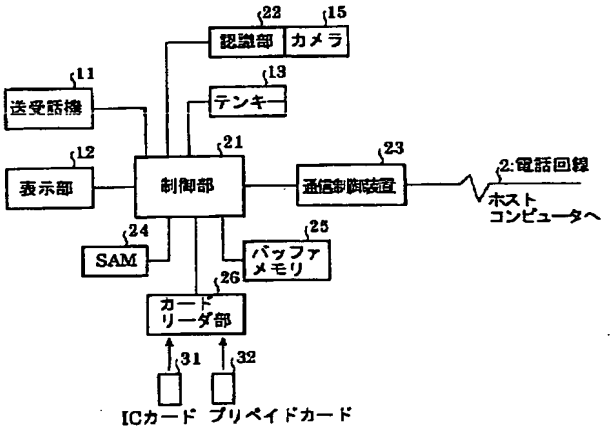
２２　認識部

４１　ホストコンピュータ

５１　パーソナルコンピュータ

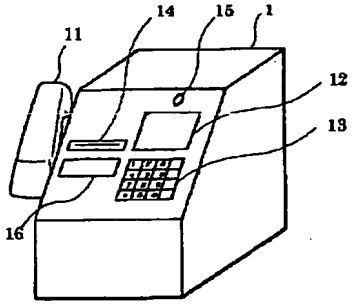
５６　ＩＣカードリーダライタ

【図１】



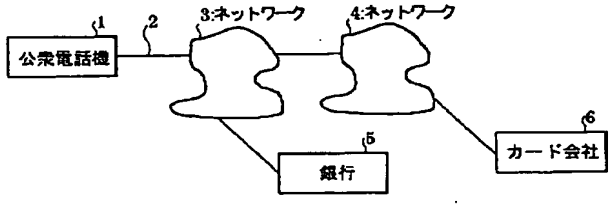
具体例１の構成を示すブロック図

【図２】



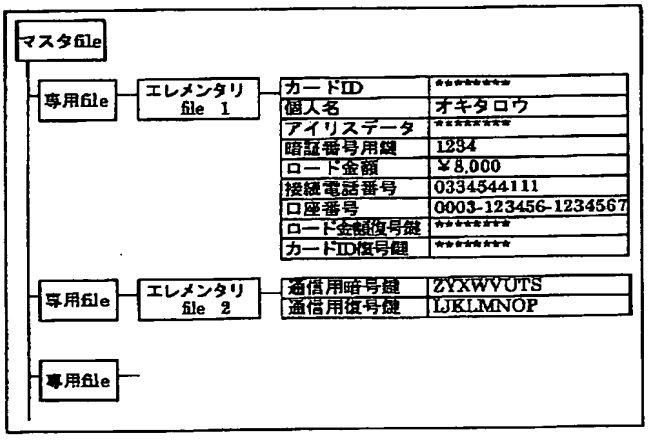
具体例１の公衆電話機の外観を示す斜視図

【図３】



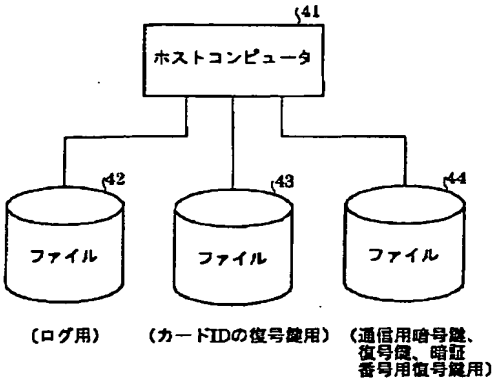
具体例１のシステム構成図

【図４】



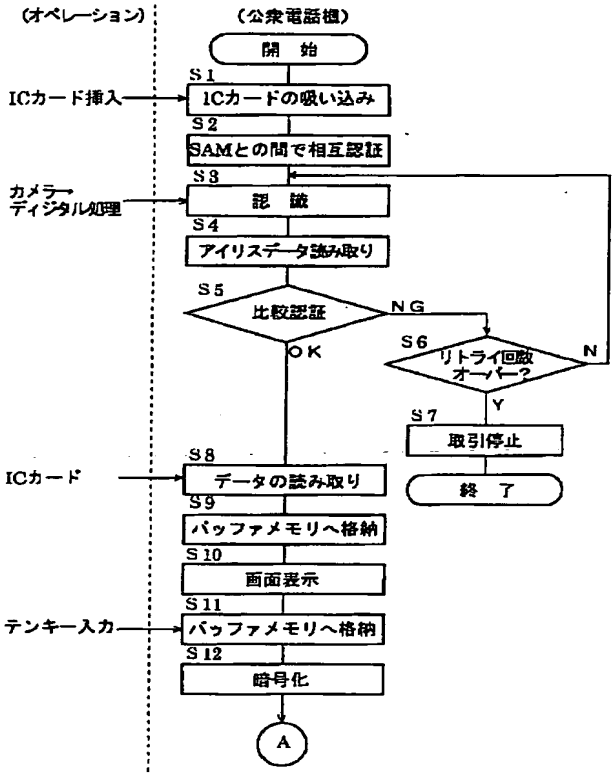
具体例１のICカードのファイル構成を示す説明図

【図５】



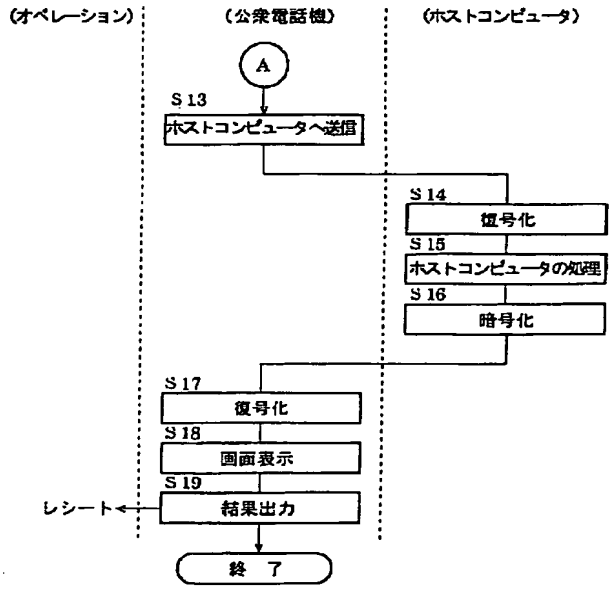
具体例１のホストコンピュータの構成を示すブロック図

【図６】



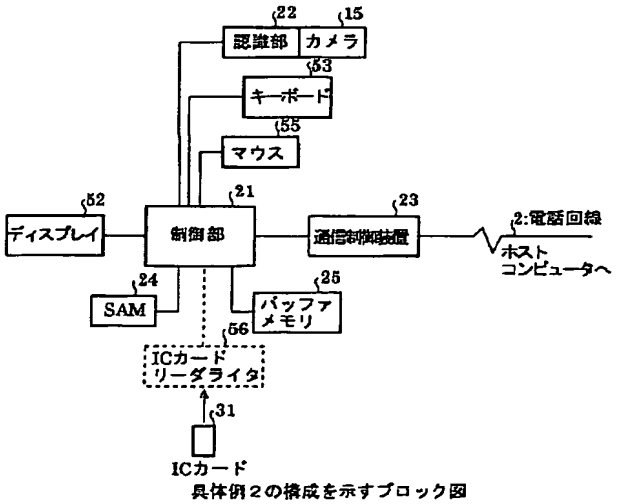
具体例１の動作を示すフローチャート（その１）

【図７】



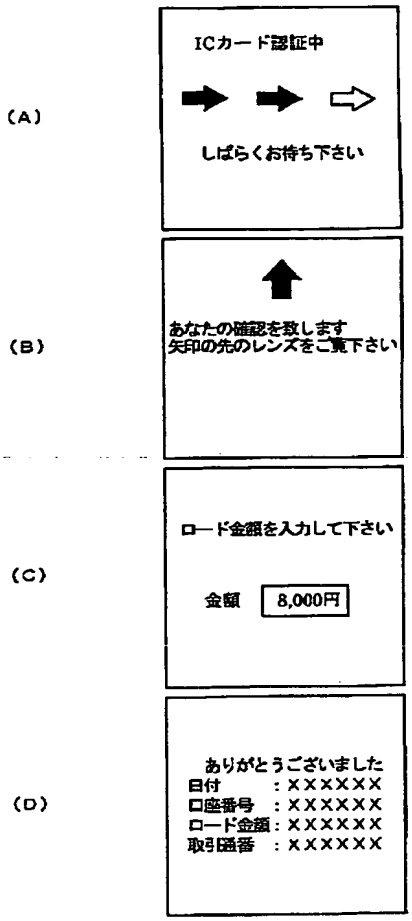
具体例１の動作を示すフローチャート（その２）

【図１１】



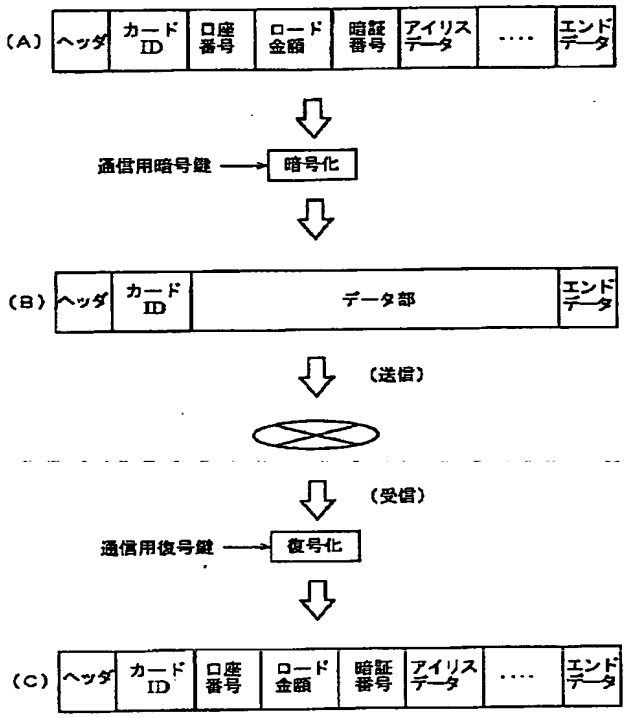
具体例２の構成を示すブロック図

【図８】



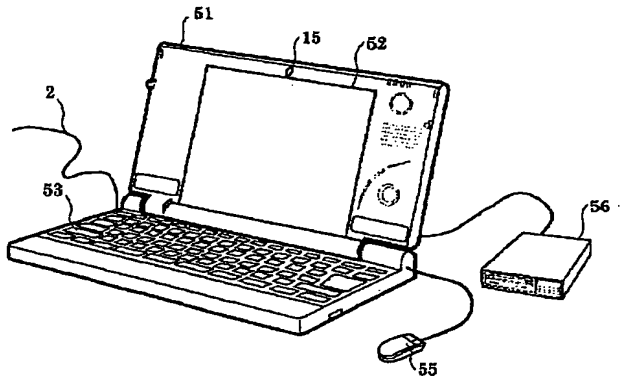
具体例１の公衆電話機の表示部に表示するメッセージの説明図

【図９】



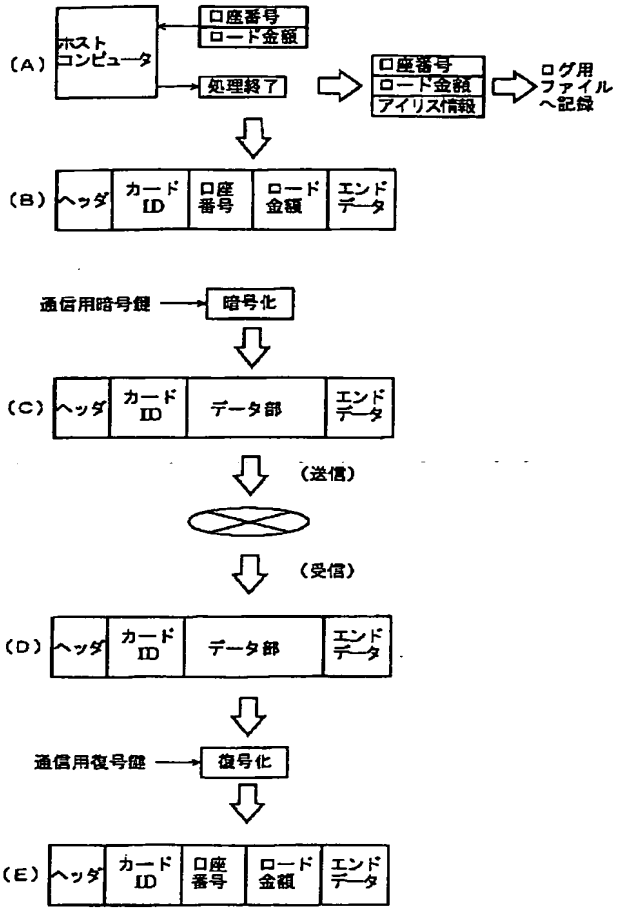
具体例１の動作説明図（その１）

【図１２】



具体例２のシステムの外観を示す斜視図

【図１０】



具体例１の動作説明図（その２）

フロントページの続き

(51) Int. Cl.[7]		識別記号	FI		テーマコード（参考）
Ｈ０４Ｍ	11/00	３０２	Ｇ０６Ｆ	15/30	Ｍ　５Ｋ０２５
	15/00				Ｃ　５Ｋ１０１
					３４０　９Ａ００１
					３５０Ａ
				15/62	４６５Ｋ

Ｆターム(参考) 3E040 AA03 CA11 CB04 DA02 DA10
FH05 FK09
5B043 AA01 AA09 BA04 CA10 DA05
FA04
5B049 AA05 BB46 CC39 DD04 EE10
EE22 EE23 FF08 GG02 GG04
GG07 GG10
5B055 BB12 BB16 CB09 EE02 EE12
EE17 EE21 EE27 FA05 HB02
HB03 HB04 JJ05 KK05 KK09
KK19 MM18 PA05 PA22 PA33
PA34 PA36
5K024 DD06 GG05
5K025 DD07
5K101 NN05 PP04
9A001 BB02 BB03 BB04 BB05 CC02
DD09 EE03 HH21 HH23 JJ08
JJ12 JJ66 JJ67 KK57 KK58
LL03